

On the calculation of the minimax-converse of the channel coding problem

Nir Elkayam Meir Feder

Department of Electrical Engineering - Systems

Tel-Aviv University, Israel

Email: nirelkayam@post.tau.ac.il, meir@eng.tau.ac.il

Abstract

A minimax-converse has been suggested for the general channel coding problem [1]. This converse comes in two flavors. The first flavor is generally used for the analysis of the coding problem with non-vanishing error probability and provides an upper bound on the rate given the error probability. The second flavor fixes the rate and provides a lower bound on the error probability. Both converses are given as a min-max optimization problem of an appropriate binary hypothesis testing problem. The properties of the first converse were studied in [2] and a saddle point was proved. In this paper we study the properties of the second form and prove that it also admits a saddle point. Moreover, an algorithm for the computation of the saddle point, and hence the bound, is developed. In the DMC case, the algorithm runs in a polynomial time.

I. INTRODUCTION

Achievable and Converse bounds were derived in [3] for the problem of point to point (P2P) channel coding by using the standard **random coding** argument. The setting considered a general channel and a general (possibly mismatched) decoding metric. Both achievable and converse results were given in terms of a function $F(R)$, which is the cumulative distribution function (CDF) of the pairwise error probability. When the decoding metric is matched to the channel (which is the focus of this paper), the converse bound reduces to the **minimax converse**, proposed in [1].

Consider an abstract channel coding problem; that is a random transformation defined by a pair of measurable spaces of inputs \mathcal{X} and outputs \mathcal{Y} and a conditional probability measure $W_{Y|X} : \mathcal{X} \mapsto \mathcal{Y}$. Let M be a positive integer. A flavor of the minimax converse is a lower bound on the error probability of any code with $M = 2^R$ codewords. The proof of the minimax converse relies on a reduction from the channel coding problem to the binary hypothesis testing problem. The bound is given in terms of $\beta_{1-\epsilon}(P, Q)$, which is the power of the test (i.e. type II error probability) at a significance level $1 - \alpha$ (i.e., type I error probability), to discriminate between probability measures P and Q .

Specifically, the minimax converse comes in the following two flavors:

$$\epsilon \geq \inf_{Q_X} \sup_{Q_Y} \beta_{1-\frac{1}{M}}(Q_X \times Q_Y, Q_X W_{Y|X}) \quad (1)$$

$$\frac{1}{M} \geq \inf_{Q_X} \sup_{Q_Y} \beta_{1-\epsilon}(Q_X W_{Y|X}, Q_X \times Q_Y). \quad (2)$$

where $Q_X W_{Y|X}$ and $Q_X \times Q_Y$ are the joint distributions on $\mathcal{X} \times \mathcal{Y}$ defined by¹:

$$\begin{aligned} (Q_X W_{Y|X})(\mathbf{x}, \mathbf{y}) &= Q_X(\mathbf{x}) W_{Y|X}(\mathbf{y}|\mathbf{x}) \\ (Q_X \times Q_Y)(\mathbf{x}, \mathbf{y}) &= Q_X(\mathbf{x}) Q_Y(\mathbf{y}) \end{aligned}$$

The first form (1) gives a lower bound on the error probability of any code given that the number of codewords is M . The second form (2) gives an upper bound on the number of codewords M given that the error probability is ϵ . Both bounds are given as a inf – sup optimization problem on the set of *input distributions* Q_X and *output distributions* Q_Y .

The functional properties of $\beta_{1-\epsilon}(Q_X W_{Y|X}, Q_X \times Q_Y)$, as a function of Q_X and Q_Y (i.e., the objective function in (2)) were investigated in [2]. In particular, the function is convex-concave and the existence of a **saddle point** was proved under general conditions. The focus of this paper is on the form (1), as this form has been used in [3] for the converse and achievable results there.

Specifically, our goal in this paper is to develop tools to evaluate the optimization problem (1), and the distributions Q_X and Q_Y that attain it. In particular, by calculating the optimal distribution Q_X in (1) for a given $R = \log M$, we obtain both a converse bound and a “good” distribution for random coding at rate R , whose performance are close up to a factor to the converse result, see [3, Theorem 4] for the exact statement.

¹throughout the paper, we assume that the alphabets \mathcal{X} and \mathcal{Y} are finite or countably infinite.

The paper is structured as follows:

- In section II we derive a general variational formula for the functional β_α . The formula is interesting by its own right (see further [4]), but in this paper we are interested only in its usage for analyzing the minimax converse.
- In section III we apply the variational formula on the functional:

$$\beta_{1-e^{-R}}(Q_X \times Q_Y, Q_X W_{Y|X}).$$

This gives us a hint for defining a new functional γ with a larger domain than β . This new functional is convex-concave, thus has a saddle point, which in turn implies a saddle point of (1). Moreover, necessary and sufficient conditions for the saddle point are proved.

- In section IV we provide a high level description of an algorithm for computing the saddle point of γ . Following that we provide in section V a more detailed description of the algorithm, showing how it builds a sequence of input distributions $Q_X^{(k)}$ using linear programs designed to reduce the score $\sup_{Q_Y} \beta_{1-e^{-R}}(Q_X^{(k)} \times Q_Y, Q_X^{(k)} W_{Y|X})$.

In the appendix C we describe the modification needed for the calculation of the minimax-converse for Discrete Memoryless Channels (DMC) where symmetries can be used to significantly reduce the computational burden into a polynomial time algorithm (as a function of the block length) for a fixed (small) $|\mathcal{X}|, |\mathcal{Y}|$ input and output alphabet.

II. GENERAL BINARY HYPOTHESIS TESTING

Recall some general (and standard) definitions about the optimal performance of a binary hypothesis testing between two probability measures P and Q over a set W :

$$\beta_\alpha(P, Q) = \min_{\substack{P_{Z|W}: \\ \sum_{w \in W} P(w) P_{Z|W}(1|w) \geq \alpha}} \sum_{w \in W} Q(w) P_{Z|W}(1|w), \quad (3)$$

where $P_{Z|W} : W \rightarrow \{0, 1\}$ is any randomized test. The minimum is guaranteed to be achieved by the Neyman–Pearson lemma. Thus, $\beta_\alpha(P, Q)$ gives the minimum probability of error under hypothesis Q if the probability of error under hypothesis P is not larger than $1 - \alpha$. β is the **power** of the test at **significance level** $1 - \alpha$.

Lemma 1. *The following variational formula holds:*

$$\beta_\alpha(P, Q) = \max_{\lambda} \left(\sum_{w \in W} \min(Q(w), \lambda P(w)) - \lambda(1 - \alpha) \right). \quad (4)$$

Moreover,

$$\beta_\alpha(P, Q) = \sum_{w \in W} \min(Q(w), \lambda P(w)) - \lambda(1 - \alpha) \quad (5)$$

If and only if:

$$P \left\{ w : \frac{Q(w)}{P(w)} < \lambda \right\} \leq \alpha \leq P \left\{ w : \frac{Q(w)}{P(w)} \leq \lambda \right\} \quad (6)$$

The proof appears in Appendix A.

III. ANALYSIS OF THE MINIMAX-CONVERSE

A. General definitions

Consider an abstract channel coding problem; that is, a random transformation defined by a pair of measurable spaces of inputs \mathcal{X} and outputs \mathcal{Y} and a conditional probability measure $W_{Y|X} : \mathcal{X} \mapsto \mathcal{Y}$. The notation $\mathcal{P}(\mathcal{A})$ stands for the set of all probability distributions on \mathcal{A} . Throughout this paper we assume that $|\mathcal{X}| < \infty, |\mathcal{Y}| < \infty$. We use max and min instead of sup and inf as we generally deal with convex/concave optimization problems over compact spaces and the sup / inf is generally attained by some element. For a distribution $Q_X \in \mathcal{P}(\mathcal{X})$ and $Q_Y \in \mathcal{P}(\mathcal{Y})$, denote by $Q_X W_{Y|X}$ the joint distribution on $\mathcal{X} \times \mathcal{Y}$ where $(Q_X W_{Y|X})(\mathbf{x}, \mathbf{y}) = Q_X(\mathbf{x}) W_{Y|X}(\mathbf{y}|\mathbf{x})$ and $(Q_X \times Q_Y)(\mathbf{x}, \mathbf{y}) = Q_X(\mathbf{x}) Q_Y(\mathbf{y})$.

B. The minimax-converse

As noted above, Polyanskiy *et al.* [1] proved the following general converse result for the average error probability that come in two flavors: For any code with M equiprobable codewords:

$$\epsilon \geq \inf_{Q_X} \sup_{Q_Y} \beta_{1-\frac{1}{M}}(Q_X \times Q_Y, Q_X W_{Y|X}) \quad (7)$$

$$\frac{1}{M} \geq \inf_{Q_X} \sup_{Q_Y} \beta_{1-\epsilon}(Q_X W_{Y|X}, Q_X \times Q_Y). \quad (8)$$

where ϵ is the average error probability. Eq. (7) gives a lower bound on the error probability in terms of the rate while the second flavor, (8), gives an upper bound on the rate in terms of the error probability. Furthermore, using equation (8) and instantiating Q_Y , it was shown in [1] that most other known converses of the channel coding problem can be derived from this converse. In [2], the functional properties of the minimax-converse (8) have been further investigated. In particular, its convexity w.r.t Q_X and concavity w.r.t Q_Y were shown.

In this paper our focus is on the form (7) as this form has been used in [3] for the achievable and converse parts. The convexity of (7) in Q_X follows from [2, Theorem 6]; however, the functional is not concave with respect to Q_Y in general. Applying Lemma 1 to this case gives the following formula:

$$\beta_{1-e^{-R}}(Q_X Q_Y, Q_X W_{Y|X}) = \max_{\lambda} \left(\sum_{\mathbf{x}, \mathbf{y}} Q_X(\mathbf{x}) \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \lambda Q_Y(\mathbf{y})) - e^{-R} \lambda \right)$$

The convexity of $\beta_{1-e^{-R}}(Q_X Q_Y, Q_X W_{Y|X})$ with respect to Q_X then follows easily since it is the max of the convex (affine) function of Q_X . Unfortunately, β is not concave in Q_Y . Yet, in order to analyze the minimax converse, we define a new function γ over a larger domain, which (as shown below) is convex-concave:

Definition 1. For any distribution $Q_X \in \mathcal{P}(\mathcal{X})$ and $\mathbf{z} = (\mathbf{z}_y) \in [0, 1]^{|\mathcal{Y}|} = \{(\mathbf{z}_y) \in \mathbb{R}^{|\mathcal{Y}|} : 0 \leq \mathbf{z}_y \leq 1\}^2$:

$$\gamma_{1-e^{-R}}(Q_X, \mathbf{z}, W_{Y|X}(\mathbf{y}|\mathbf{x})) = \sum_{\mathbf{x}, \mathbf{y}} Q_X(\mathbf{x}) \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y) - e^{-R} \sum_{\mathbf{y}} \mathbf{z}_y \quad (9)$$

Since throughout this paper $W_{Y|X}(\mathbf{y}|\mathbf{x})$ and R are held fixed, we will abbreviate and write $\gamma(Q_X, \mathbf{z})$ instead of $\gamma_{1-e^{-R}}(Q_X, \mathbf{z}, W_{Y|X}(\mathbf{y}|\mathbf{x}))$.

Some properties of $\gamma(Q_X, \mathbf{z})$ are summarized in the following theorem. In particular, the functional admits a saddle point.

Theorem 1.

$\gamma(Q_X, \mathbf{z})$ is convex in Q_X , concave in \mathbf{z} and admits a saddle point (Q_X^*, \mathbf{z}^*) , i.e.

$$\gamma(Q_X^*, \mathbf{z}) \leq \gamma(Q_X^*, \mathbf{z}^*) \leq \gamma(Q_X, \mathbf{z}^*) \quad (10)$$

for all Q_X, \mathbf{z} . In particular:

$$\epsilon = \min_{Q_X} \max_{\mathbf{z}} \gamma(Q_X, \mathbf{z}) = \max_{\mathbf{z}} \min_{Q_X} \gamma(Q_X, \mathbf{z}) \quad (11)$$

Moreover, for \mathbf{x} such that $Q_X^*(\mathbf{x}) > 0$ we have:

$$\epsilon = \sum_{\mathbf{y}} \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y^*) - e^{-R} \sum_{\mathbf{y}} \mathbf{z}_y^* \quad (12)$$

and for \mathbf{x} such that $Q_X^*(\mathbf{x}) = 0$:

$$\epsilon \leq \sum_{\mathbf{y}} \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y^*) - e^{-R} \sum_{\mathbf{y}} \mathbf{z}_y^* \quad (13)$$

Proof: Note that both Q_X and \mathbf{z} range over convex compact sets and that $\gamma(Q_X, \mathbf{z})$ is a convex-concave functional (affine in $Q(\mathbf{x})$ and concave in \mathbf{z} by the concavity of the min function) and $\gamma(Q_X, \mathbf{z})$ is continuous in both arguments. The existence of the saddle point and (11) follow from the Fan's minimax theorem [5].

By the saddle point property:

$$\epsilon = \gamma(Q_X^*, \mathbf{z}^*) = \min_{Q_X} \gamma(Q_X, \mathbf{z}^*)$$

²Throughout this paper \mathbf{z} will stand for a vector, indexed by the elements \mathcal{Y} , i.e., the component of \mathbf{z} are \mathbf{z}_y .

Note that:

$$\gamma(Q_X, \mathbf{z}) = \sum_{\mathbf{x}} Q_X(\mathbf{x}) \left(\sum_{\mathbf{y}} \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_{\mathbf{y}}) - e^{-R} \sum_{\mathbf{y}} \mathbf{z}_{\mathbf{y}} \right)$$

and:

$$\begin{aligned} \min_{Q_X} \gamma(Q_X, \mathbf{z}^*) &= \min_{Q_X} \left\{ \sum_{\mathbf{x}} Q_X(\mathbf{x}) \left(\sum_{\mathbf{y}} \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_{\mathbf{y}}^*) - e^{-R} \sum_{\mathbf{y}} \mathbf{z}_{\mathbf{y}}^* \right) \right\} \\ &= \min_{\mathbf{x} \in \mathcal{X}} \left\{ \sum_{\mathbf{y}} \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_{\mathbf{y}}^*) - e^{-R} \sum_{\mathbf{y}} \mathbf{z}_{\mathbf{y}}^* \right\} \end{aligned} \quad (14)$$

hence (12) and (13) follow from the linearity of $\gamma(Q_X, \mathbf{z})$ in Q_X . ■

The next theorem presents the connection between $\gamma(Q_X, \mathbf{z})$ and $\beta_{1-e^{-R}}(Q(\mathbf{x})Q(\mathbf{y}), Q(\mathbf{x})W_{Y|X}(\mathbf{y}|\mathbf{x}))$.

Theorem 2.

For any distribution Q_X the following holds:

$$\max_{Q_Y} \beta_{1-e^{-R}}(Q_X \times Q_Y, Q_X W_{Y|X}) = \max_{\mathbf{z}} \gamma(Q_X, \mathbf{z}) \quad (15)$$

Moreover, \mathbf{z}^* attains the maximum in (15) if and only if for each \mathbf{y} :

$$Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_{\mathbf{y}}^* \} \leq e^{-R} \leq Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_{\mathbf{y}}^* \} \quad (16)$$

Proof: (15) follows from:

$$\begin{aligned} \max_{Q_Y} \beta_{1-e^{-R}}(Q_X \times Q_Y, Q_X W_{Y|X}) &= \max_{Q_Y} \max_{\lambda} \left(\sum_{\mathbf{x}, \mathbf{y}} Q_X(\mathbf{x}) \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \lambda Q_Y(\mathbf{y})) - e^{-R} \lambda \right) \\ &= \max_{\mathbf{z}} \left(\sum_{\mathbf{x}, \mathbf{y}} Q_X(\mathbf{x}) \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_{\mathbf{y}}) - e^{-R} \sum_{\mathbf{y}} \mathbf{z}_{\mathbf{y}} \right) \end{aligned}$$

where we write $\mathbf{z}_{\mathbf{y}} = \lambda Q_Y(\mathbf{y})$ and use $\lambda = \sum_{\mathbf{y}} \mathbf{z}_{\mathbf{y}}$. Note that to attain the maximum, we can restrict $\mathbf{z}_{\mathbf{y}} \leq 1$ since $\gamma(Q_X, \mathbf{z}) \leq \gamma(Q_X, \min(\mathbf{z}, 1))$. To prove (16):

$$\begin{aligned} \gamma(Q_X, \mathbf{z}) &= \sum_{\mathbf{x}, \mathbf{y}} Q_X(\mathbf{x}) \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_{\mathbf{y}}) - e^{-R} \sum_{\mathbf{y}} \mathbf{z}_{\mathbf{y}} \\ &= \sum_{\mathbf{y}} \left(\sum_{\mathbf{x}} \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_{\mathbf{y}}) Q_X(\mathbf{x}) - e^{-R} \mathbf{z}_{\mathbf{y}} \right) \\ &= \sum_{\mathbf{y}} \left(\sum_{\mathbf{x}} \min(W_{X|Y}(\mathbf{x}|\mathbf{y}), \mathbf{z}_{\mathbf{y}}) Q_Y(\mathbf{y}) - e^{-R} \mathbf{z}_{\mathbf{y}} \right) \\ &= \sum_{\mathbf{y}} \left(\sum_{\mathbf{x}} Q_Y(\mathbf{y}) \min \left(W_{X|Y}(\mathbf{x}|\mathbf{y}), \frac{\mathbf{z}_{\mathbf{y}}}{Q_Y(\mathbf{y})} Q_X(\mathbf{x}) \right) - e^{-R} \mathbf{z}_{\mathbf{y}} \right) \\ &= \sum_{\mathbf{y}} Q_Y(\mathbf{y}) \left(\sum_{\mathbf{x}} \min \left(W_{X|Y}(\mathbf{x}|\mathbf{y}), \frac{\mathbf{z}_{\mathbf{y}}}{Q_Y(\mathbf{y})} Q_X(\mathbf{x}) \right) - e^{-R} \frac{\mathbf{z}_{\mathbf{y}}}{Q_Y(\mathbf{y})} \right) \end{aligned}$$

where we assumed $Q_Y(\mathbf{y}) > 0$ for all \mathbf{y} to avoid cumbersome notation.

$$\begin{aligned} \sup_{\mathbf{z}} \gamma(Q_X, \mathbf{z}) &= \sup_{\mathbf{z}} \sum_{\mathbf{y}} Q_Y(\mathbf{y}) \left(\sum_{\mathbf{x}} \min \left(W_{X|Y}(\mathbf{x}|\mathbf{y}), \frac{\mathbf{z}_{\mathbf{y}}}{Q_Y(\mathbf{y})} Q_X(\mathbf{x}) \right) - e^{-R} \frac{\mathbf{z}_{\mathbf{y}}}{Q_Y(\mathbf{y})} \right) \\ &= \sum_{\mathbf{y}} Q_Y(\mathbf{y}) \sup_{\mathbf{z}_{\mathbf{y}}} \left(\sum_{\mathbf{x}} \min \left(W_{X|Y}(\mathbf{x}|\mathbf{y}), \frac{\mathbf{z}_{\mathbf{y}}}{Q_Y(\mathbf{y})} Q_X(\mathbf{x}) \right) - e^{-R} \frac{\mathbf{z}_{\mathbf{y}}}{Q_Y(\mathbf{y})} \right) \\ &= \sum_{\mathbf{y}} Q_Y(\mathbf{y}) \beta_{1-e^{-R}}(Q_X, W_{X|Y}) \end{aligned}$$

Moreover, the optimal \mathbf{z}_y must satisfy condition (6):

$$Q_X \left\{ \mathbf{x} : \frac{W(\mathbf{x}|\mathbf{y})}{Q(\mathbf{x})} < \frac{\mathbf{z}_y}{Q(\mathbf{y})} \right\} \leq 1 - e^{-R} \leq Q_X \left\{ \mathbf{x} : \frac{W(\mathbf{x}|\mathbf{y})}{Q(\mathbf{x})} \leq \frac{\mathbf{z}_y}{Q(\mathbf{y})} \right\}$$

which gives (16) after rearranging the terms. ■

Remark 1. Combining the last theorem with (14) we recover the formula that appears in [6, Proposition 14] where it was proven by indirect arguments relying on the duality in linear programming.

Theorems 1 and 2 provide necessary conditions, (12),(13) and (16) for the saddle point Q_X^* and \mathbf{z}^* . The following theorem shows that these conditions are also sufficient.

Theorem 3. Any distribution Q_X^* and \mathbf{z}^* satisfy conditions (12) and (13) and (16) is a saddle point of $\gamma(Q_X, \mathbf{z})$.

Proof: We need to show that:

$$\gamma(Q_X^*, \mathbf{z}) \leq \gamma(Q_X^*, \mathbf{z}^*) \leq \gamma(Q_X, \mathbf{z}^*)$$

The left hand side follows from (16) and the right hand side from (12),(13) and the linearity in Q_X . ■

IV. AN ALGORITHM FOR THE COMPUTATION OF THE SADDLE POINT - HIGH LEVEL DESCRIPTION

In the following sections we present our algorithm for the computation of the saddle point. We first give a high level review of the ingredients of the algorithm.

The general idea is to generate a sequence $(Q_X^{(k)}, \mathbf{z}^{(k)})$ such that:

$$\gamma(Q_X^{(k)}, \mathbf{z}^{(k)}) = \max_{\mathbf{z}} \gamma(Q_X^{(k)}, \mathbf{z}) > \max_{\mathbf{z}} \gamma(Q_X^{(k+1)}, \mathbf{z}) = \gamma(Q_X^{(k+1)}, \mathbf{z}^{(k+1)})$$

The initial step takes any distribution $Q_X^{(0)}$ and calculate $\mathbf{z}^{(0)}$ using (16). Then, each iteration contains two steps as we now describe:

A. Optimizing $Q_X^{(k+1)}$ for a given $\mathbf{z}^{(k)}$

Given $\mathbf{z}^{(k)}$ we can find a distribution $Q_X^{(k+1)}$ that minimizes $\gamma(Q_X, \mathbf{z}^{(k)})$ subject to condition (16). This is a linear program with $|\mathcal{X}|$ variables, $2 \cdot |\mathcal{Y}| + |\mathcal{X}|$ linear inequalities, $(2 \cdot |\mathcal{Y}|$ for (16) and $|\mathcal{X}|$ for the nonnegativity of $Q_X(\mathbf{x})$), and additional equality for $Q_X(\mathbf{x})$ to sum to 1. If:

$$\min_{Q_X} \gamma(Q_X, \mathbf{z}^{(k)}) < \gamma(Q_X^{(k)}, \mathbf{z}^{(k)})$$

Then we define:

- 1) $\mathbf{z}^{(k+1)} = \mathbf{z}^{(k)}$
- 2) $Q_X^{(k+1)} = \arg \min_{Q_X} \gamma(Q_X, \mathbf{z}^{(k)})$

We will refer to this stage as a **local linear optimization** and say that $Q_X^{(k+1)}$ is **locally optimal** given $\mathbf{z}^{(k)}$.

B. Improving a locally optimal solution

When we hold a locally optimal solution $Q_X^{(k)}$, we have to change $\mathbf{z}^{(k)}$ in order to improve (reduce) the current score (i.e., $\gamma(Q_X^{(k)}, \mathbf{z}^{(k)})$). Consider any perturbation μ on Q_X , i.e., $\sum_{\mathbf{x}} \mu(\mathbf{x}) = 0$, and let $Q_X^\mu = Q_X^{(k)} + \delta\mu$ where δ is small enough.³ For Q_X^μ , let \mathbf{z}^μ satisfy the condition (16) with respect to Q_X^μ . Let:

$$\eta(\mu) = \frac{\gamma(Q_X^\mu, \mathbf{z}^\mu) - \gamma(Q_X^{(k)}, \mathbf{z}^{(k)})}{\delta} \quad (17)$$

If $\min_{\mu} \eta(\mu) = 0$ then we cannot improve $Q_X^{(k)}$ and we have a **globally optimal solution**. If $\eta(\mu) < 0$ for some μ , then we found an improvement of the score function and we define:

- 1) $\mathbf{z}^{(k+1)} = \mathbf{z}^\mu$
- 2) $Q_X^{(k+1)} = Q_X^\mu$

In practice we will show that the problem of minimizing (17) can be translated to a linear program as well (up to some regularities that we will have to handle separately), which will allow us to solve it.

³Note that when $Q_X(\mathbf{x}) = 0$ we must take $\mu(\mathbf{x}) \geq 0$ and if $Q_X(\mathbf{x}) = 1$ we must take $\mu(\mathbf{x}) < 0$

V. IMPROVING A LOCALLY OPTIMAL SOLUTION - DETAILS

In this section we describe in detail how to implement step B of the iteration, described above in high level.

Fix Q_X and \mathbf{z} and assume the Q_X is locally optimal with respect to \mathbf{z} . Let μ be a perturbation of Q_X , i.e., $\mu \in \mathbb{R}^{|\mathcal{X}|}$ with $\sum_{\mathbf{x}} \mu(\mathbf{x}) = 0$. Recall that by (16) for each y we have:

$$Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} \leq e^{-R} \leq Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}$$

Assume initially that $Q_X(\mathbf{x}) > 0$ for all \mathbf{x} . We point out in the sequel where we need this assumption. When we do have zeros in the distribution $Q_X(\mathbf{x})$ we will restrict ourselves to the subset: $\{ \mathbf{x} \in \mathcal{X} : Q_X(\mathbf{x}) > 0 \}$. In subsection V-H we explain how to recover from this assumption.

A. Notation

We will make use of the following notation through this section.

- 1) $\mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y\}}$ denotes a vector, indexed by \mathbf{x} with $\mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y\}}(\mathbf{x}) = 1$ if $W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y$ and 0 otherwise. Define $\mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y\}}$ likewise.
- 2) $\mu^T \cdot L$ is the scalar product between the vectors μ and L , i.e.: $\mu^T \cdot L = \sum_{\mathbf{x}} \mu(\mathbf{x}) L(\mathbf{x})$.

B. Phase I: Changing \mathbf{z} to achieve strict inequality on the left hand side of (16)

Throughout, we assume that:

$$\begin{aligned} Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} &< e^{-R} \\ &\leq Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \} \end{aligned}$$

i.e., we have strict inequality on the left hand side of (16). If this is not the case, we can change \mathbf{z}_y until this is valid for all y .

If $Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} = e^{-R}$, Let:

$$\mathbf{x}_y = \arg \min_{\mathbf{x}} \{ W_{Y|X}(\mathbf{y}|\mathbf{x}) : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y, Q_X(\mathbf{x}) > 0 \}$$

Then:

- $Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} = Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq W_{Y|X}(\mathbf{y}|\mathbf{x}_y) \}$
- $Q_X(\mathbf{x}_y) > 0$
- $Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > W_{Y|X}(\mathbf{y}|\mathbf{x}_y) \} < e^{-R}$ since $Q_X(\mathbf{x}_y) > 0$.

Replacing \mathbf{z}_y with $W_{Y|X}(\mathbf{y}|\mathbf{x}_y)$ we have strict inequality on the left hand side in (16) and we haven't changed the local optimality since the optimality condition (16) still holds by construction.

C. Phase II: Compute Alternative \mathbf{z} with strict inequality on the right hand side of (16)

Following the same reasoning, we can find $\mathbf{z}_y^l \leq \mathbf{z}_y$ that also satisfy (16) with the following additional properties:

- If $Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} < e^{-R} < Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}$ then $\mathbf{z}_y^l = \mathbf{z}_y$.
- $Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y^l \} \leq e^{-R} < Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y^l \}$
- If $Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y^l \} = e^{-R} = Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}$ then: $\mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y^l\}} = \mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y\}}$.

In order for the last equality to hold we must assume that: $Q_X(\mathbf{x}) > 0$ for all \mathbf{x} .

D. Phase III: Compute \mathbf{z}^μ

Let $Q_X^\mu = Q_X + \delta \cdot \mu$ where δ is sufficiently small. Recall that we must find \mathbf{z}^μ that satisfies the condition (16) with respect to Q_X^μ . From:

$$Q_X^\mu \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} = Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} + \delta \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \}}$$

we always have

$$Q_X^\mu \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} < e^{-R}$$

for sufficiently small δ and:

$$Q_X^\mu \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \} \geq e^{-R} \Leftrightarrow \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}} \geq 0$$

Hence when $\mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}} < 0$ we must change \mathbf{z}_y since it does not satisfy condition (16) anymore. Since:

$$Q_X^\mu \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y^l \} > e^{-R}$$

for sufficiently small δ and:

$$Q_X^\mu \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y^l \} \leq e^{-R} \Leftrightarrow \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y^l \}} \leq 0$$

Now, from $\mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y^l \}} = \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}}$ we have:

$$\mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y^l \}} = \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}}$$

and when $\mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}} < 0$ we can take \mathbf{z}_y^l .

To summarize, let:

$$\mathbf{z}_y^\mu = \begin{cases} \mathbf{z}_y & \text{if } \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}} \geq 0 \\ \mathbf{z}_y^l & \text{if } \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}} < 0 \end{cases} \quad (18)$$

Then \mathbf{z}^μ satisfies (16) with respect to Q_X^μ for δ sufficiently small.

E. Computation of $\gamma(Q_X^\mu, \mathbf{z}^\mu)$

Let:

$$\eta(\mu, \mathbf{z}) \triangleq \sum_{\mathbf{x}, \mathbf{y}} \mu(\mathbf{x}) \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y) \quad (19)$$

We have:

$$\begin{aligned} \gamma(Q_X^\mu, \mathbf{z}^\mu) &= \sum_{\mathbf{x}, \mathbf{y}} (Q_X(\mathbf{x}) + \delta \mu(\mathbf{x})) \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y^\mu) \\ &\quad - e^{-R} \sum_{\mathbf{y}} \mathbf{z}_y^\mu \\ &= \gamma(Q_X, \mathbf{z}^\mu) + \delta \sum_{\mathbf{x}, \mathbf{y}} \mu(\mathbf{x}) \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y^\mu) \\ &= \gamma(Q_X, \mathbf{z}^\mu) + \delta \eta(\mu, \mathbf{z}^\mu) \end{aligned}$$

Since \mathbf{z}^μ also satisfies (16) with respect to Q_X , $\gamma(Q_X, \mathbf{z}^\mu) = \gamma(Q_X, \mathbf{z})$ and:

$$\begin{aligned} \frac{\gamma(Q_X^\mu, \mathbf{z}^\mu) - \gamma(Q_X, \mathbf{z})}{\delta} &= \frac{\gamma(Q_X^\mu, \mathbf{z}^\mu) - \gamma(Q_X, \mathbf{z}^\mu)}{\delta} \\ &= \eta(\mu, \mathbf{z}^\mu) \end{aligned}$$

and:

$$\begin{aligned} \eta(\mu, \mathbf{z}^\mu) - \eta(\mu, \mathbf{z}) &= \sum_{\mathbf{x}, \mathbf{y}} \mu(\mathbf{x}) (\min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y^\mu) - \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y)) \\ &= \sum_{\mathbf{y} : \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}} < 0} \sum_{\mathbf{x}} (\min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y^l) - \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y)) \\ &\stackrel{(a)}{=} \sum_{\mathbf{y} : \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}} < 0} (\mathbf{z}_y^l - \mathbf{z}_y) \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}} \\ &= \sum_{\mathbf{y}} (\mathbf{z}_y^l - \mathbf{z}_y) \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}} \mathbb{1}_{\{ \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}} < 0 \}} \end{aligned}$$

where (a) follows from:

$$\begin{aligned} &\sum_{\mathbf{x}} (\min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y^l) - \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y)) \\ &= \sum_{\mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y^l} \mathbf{z}_y^l + \sum_{\mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \leq \mathbf{z}_y^l} W_{Y|X}(\mathbf{y}|\mathbf{x}) - \sum_{\mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y} W_{Y|X}(\mathbf{y}|\mathbf{x}) - \sum_{\mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) < \mathbf{z}_y} \mathbf{z}_y \\ &= (\mathbf{z}_y^l - \mathbf{z}_y) \mu^T \cdot \mathbb{1}_{\{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}} \end{aligned} \quad (20)$$

since $\mathbb{1}_{\{\mathbf{x}: W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y^l\}} = \mathbb{1}_{\{\mathbf{x}: W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y\}}$ and also $\mathbb{1}_{\{\mathbf{x}: W_{Y|X}(\mathbf{y}|\mathbf{x}) \leq \mathbf{z}_y^l\}} = \mathbb{1}_{\{\mathbf{x}: W_{Y|X}(\mathbf{y}|\mathbf{x}) < \mathbf{z}_y\}}$. To sum until here:

$$\eta(\mu, \mathbf{z}^\mu) = \eta(\mu, \mathbf{z}) - \sum_{\mathbf{y}} (\mathbf{z}_{\mathbf{y}} - \mathbf{z}_{\mathbf{y}}^l) \mu^T \cdot \mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_{\mathbf{y}}\}} \mathbb{1}_{\{\mu^T \cdot \mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_{\mathbf{y}}\}} < 0\}} \quad (21)$$

And we want to optimize $\eta(\mu, \mathbf{z}^\mu)$ with respect to μ .

F. Optimize for μ

Let define:

- $b(\mathbf{x}) = \sum_{\mathbf{y}} \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_{\mathbf{y}})$ so that: $\eta(\mu, \mathbf{z}) = \mu^T \cdot b$
- $a_y = \mathbb{1}_{\{\mathbf{x}: W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_{\mathbf{y}}\}}$
- $\alpha_y = \mathbf{z}_{\mathbf{y}} - \mathbf{z}_{\mathbf{y}}^l \geq 0$

Then:

$$\eta(\mu, \mathbf{z}^\mu) = \eta(\mu) = \mu^T \cdot \left(b - \sum_{\mathbf{y}} \alpha_y a_y \mathbb{1}_{\{\mu^T \cdot a_y < 0\}} \right) \quad (22)$$

In appendix B we prove the following two lemmas. The first shows how to translate the problem of minimizing $\eta(\mu)$ into a linear program. We provide these lemmas here using the notation used in this section. (i.e., index the vectors with y)

Lemma 2. *Let:*

$$\eta(\mu) = \mu^T \cdot \left(b - \sum_{\mathbf{y}} \alpha_y a_y \mathbb{1}_{\{\mu^T \cdot a_y < 0\}} \right) \quad (23)$$

Then minimization of $\eta(\mu)$ subject to $\mu^T \cdot \mathbf{1} = 0$ is equivalent to the following linear program:

$$\min \begin{pmatrix} \mu \\ z \end{pmatrix}^T \cdot \begin{pmatrix} b \\ \alpha \end{pmatrix} \text{ s.t. } \begin{pmatrix} \mu \\ z \end{pmatrix}^T \cdot \begin{pmatrix} A & 0 \\ I & I \end{pmatrix} \geq 0, \mu^T \cdot \mathbf{1} = 0 \quad (24)$$

where A is the matrix with columns a_y , α is a vector with entries α_y , and $\mathbf{1}$ is the all-one vector.

The next lemma provides necessary and sufficient conditions for $\mu = 0$ to be the optimal minimizer of $\eta(\mu)$.

Lemma 3 (Generalized Farkas). *Let $a_y \in \mathbb{R}^n$, $y \in \mathcal{Y}$, $b \in \mathbb{R}^{|\mathcal{X}|}$ and $\alpha_y \geq 0$. Then*

$$\mu^T \cdot \left(b - \sum_{\mathbf{y}} \alpha_y a_y \mathbb{1}_{\{\mu^T \cdot a_y < 0\}} \right) \geq 0 \quad (25)$$

for all $\mu \in \mathbb{R}^{|\mathcal{X}|}$ such that $\mu^T \cdot \mathbf{1} = 0$ if and only if:

$$b = \sum_j \lambda_j a_j + \tau \mathbf{1}, 0 \leq \lambda_j \leq \alpha_j, \tau \in \mathbb{R} \quad (26)$$

If $\eta(\mu) < 0$ then we have found an improvement of the score and we can keep on going to find a new locally optimal solution.

G. The case where $\min_{\mu} \eta(\mu) = 0$

If $\eta(\mu) = 0$ is the minimal value, then we cannot improve on the current solution using perturbation that consider non-zeros elements of $Q_X(\mathbf{x})$. (The case where there are zeros in $Q_X(\mathbf{x})$ is discussed in subsection V-H).

Let us show that indeed in this case we reached the optimal solution, i.e., we can recover the conditions (12) and (13).

Define \mathbf{z}^o by: $\mathbf{z}_y^o = \mathbf{z}_{\mathbf{y}} - \lambda_y$. Then:

- 1) $\mathbf{z}_{\mathbf{y}}^l \leq \mathbf{z}_{\mathbf{y}}^o \leq \mathbf{z}_{\mathbf{y}}$
- 2) $b^o(\mathbf{x}) = \sum_{\mathbf{y}} \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_{\mathbf{y}}^o) = \tau$, i.e. $b^o = \tau \mathbf{1}$

The last equality follows from:

$$\begin{aligned} \mu^T \cdot (b^o - b) &= \sum_{\mathbf{y}} \sum_{\mathbf{x}} \mu(\mathbf{x}) (\min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_{\mathbf{y}}^o) - \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_{\mathbf{y}})) \\ &\stackrel{(a)}{=} \sum_{\mathbf{y}} (\mathbf{z}_{\mathbf{y}}^o - \mathbf{z}_{\mathbf{y}}) \mu^T \cdot \mathbb{1}_{\{\mathbf{x}: W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_{\mathbf{y}}\}} \\ &= - \sum_{\mathbf{y}} \lambda_y \mu^T \cdot a_y \end{aligned}$$

where (a) follows from the same reasoning as (20). Hence:

$$b^o = b - \sum_y \lambda_y a_y = \tau e$$

H. Zeros in $Q_X(\mathbf{x})$

Let Q_X, \mathbf{z} be such that:

$$Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} \leq e^{-R} \leq Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \}$$

$$\epsilon = \sum_y \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y) - e^{-R} \sum_y \mathbf{z}_y$$

for all \mathbf{x} with $Q_X(\mathbf{x}) > 0$, and:

$$\epsilon > \sum_y \min(W_{Y|X}(\mathbf{y}|\mathbf{x}_1), \mathbf{z}_y) - e^{-R} \sum_y \mathbf{z}_y$$

for some \mathbf{x}_1 with $Q_X(\mathbf{x}_1) = 0$. We also assume that Q_X is locally optimal, which means that we cannot improve the score by running a local linear program. Obviously, we cannot argue that the optimality condition (13) holds.

For any perturbation with $\mu(\mathbf{x}_1) > 0$, we must have that at least one of the linear inequality constraints is violated. Equivalently, we can say: For any perturbation that does not violate the linear inequality constraint, we must have $\mu(\mathbf{x}_1) \leq 0$.

- From $Q_X^\mu \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} = Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} + \mu^T \cdot \mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y\}}$, If $Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} = e^{-R}$ then in order not to violate the linear inequality we must have: $\mu^T \cdot \mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y\}} \leq 0$
- From $Q_X^\mu \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \} = Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \} + \mu^T \cdot \mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y\}}$, If $Q_X \{ \mathbf{x} : W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \} = e^{-R}$ then in order not to violate the linear inequality we must have: $\mu^T \cdot \mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y\}} \geq 0$
- μ must satisfy: $\mu^T \cdot \mathbf{1} = 0$.

By Farkas lemma (4) we must have:

$$\delta_{\mathbf{x}_1} = \sum_{\mathbf{y}: Q_X \{ \mathbf{x}: W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y \} = e^{-R}} \lambda_y^l \mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y\}} + \sum_{\mathbf{y}: Q_X \{ \mathbf{x}: W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y \} = e^{-R}} \lambda_y^h \mathbb{1}_{\{W_{Y|X}(\mathbf{y}|\mathbf{x}) \geq \mathbf{z}_y\}} + \alpha \mathbf{1}$$

with $\lambda_y^l \geq 0$ and $\lambda_y^h \leq 0$ and $\delta_{\mathbf{x}_1}$ is the vector with 1 at \mathbf{x}_1 and 0 otherwise.

At this point we can use these λ s by adding them to \mathbf{z}_y in order to increase score at \mathbf{x}_1 up to the other scores and meet the conditions (13) along the same lines as V-G. Note that we might not be able to do this in a single step. Moreover, we have to do this process for each variable with $Q_X(\mathbf{x}) = 0$ and lower score than the global score we have.

VI. SUMMARY

In this paper we have studied the functional properties of the minimax-converse for a fixed rate. The existence of a saddle point was proved, necessary and sufficient conditions were derived and an algorithm for the computation of the saddle point was presented. For the DMC case, the algorithm can be modified to incorporate additional linear constraints (*i.e.*, input and output distribution that are uniform on types) and this results in a polynomial time algorithm for the computation of the saddle point. The saddle point distribution can be used to optimize the random coding argument (*e.g.*, [3]).

APPENDIX A PROOF OF LEMMA 1

A. Proof of (5)

Let λ, δ be the thresholds for the optimal test, and let:

$$A = \left\{ w : \frac{Q(w)}{P(w)} < \lambda \right\}$$

$$B = \left\{ w : \frac{Q(w)}{P(w)} = \lambda \right\}$$

Then:

$$\alpha = P(A) + \delta P(B) \tag{27}$$

And:

$$\beta = Q(A) + \delta Q(B) \tag{28}$$

Multiply (27) by λ , subtract (28) and use $Q(B) = \lambda P(B)$:

$$\beta - \lambda\alpha = Q(A) - \lambda P(A)$$

On the other hand:

$$\begin{aligned} \sum_{w \in W} \min(Q(w), \lambda P(w)) &= \sum_{w \in A} Q(w) + \sum_{w \in A^c} \lambda P(w) \\ &= Q(A) + \lambda(1 - P(A)) \\ &= Q(A) - \lambda P(A) + \lambda \\ &= \beta - \lambda\alpha + \lambda \end{aligned}$$

Thus:

$$\beta = \sum_{w \in W} \min(Q(w), \lambda P(w)) - \lambda(1 - \alpha)$$

B. proof of the sup formula (smaller λ)

Note that the optimal λ satisfies the following:

$$P\left\{w : \frac{Q(w)}{P(w)} \geq \lambda\right\} \geq 1 - \alpha \geq P\left\{w : \frac{Q(w)}{P(w)} > \lambda\right\} \quad (29)$$

Let $\lambda_1 < \lambda$:

$$\begin{aligned} &\sum_{w \in W} \min(Q(w), \lambda_1 P(w)) - \sum_{w \in W} \min(Q(w), \lambda P(w)) \\ &= \sum_{w \in W: \lambda_1 P(w) < Q(w) < \lambda P(w)} (\lambda_1 P(w) - Q(w)) + (\lambda_1 - \lambda) \sum_{w \in W: \lambda P(w) \leq Q(w)} P(w) \\ &\stackrel{(a)}{\leq} (\lambda_1 - \lambda) \sum_{w \in W: \lambda P(w) \leq Q(w)} P(w) \\ &= (\lambda_1 - \lambda) P\left\{w : \frac{Q(w)}{P(w)} \geq \lambda\right\} \\ &\stackrel{(b)}{\leq} (\lambda_1 - \lambda) (1 - \alpha) \end{aligned}$$

where (a) follow from: $\lambda_1 P(w) - Q(w) < 0$, (b) follow from $\lambda_1 - \lambda < 0$ and $P\left\{w : \frac{Q(w)}{P(w)} \geq \lambda\right\} \geq 1 - \alpha$. Rearranging the terms:

$$\sum_{w \in W} \min(Q(w), \lambda_1 P(w)) - \lambda_1(1 - \alpha) \leq \sum_{w \in W} \min(Q(w), \lambda P(w)) - \lambda(1 - \alpha)$$

If λ_1 does not satisfy the condition (6), then:

- If $P\left\{w : \frac{Q(w)}{P(w)} \leq \lambda_1\right\} < P\left\{w : \frac{Q(w)}{P(w)} < \lambda\right\}$, then we are finished because there exist w_0 with $P(w_0) > 0$, $\frac{Q(w_0)}{P(w_0)} < \lambda$, and $\frac{Q(w_0)}{P(w_0)} > \lambda_1$, which gives strict inequality in (a) above.
- If $P\left\{w : \frac{Q(w)}{P(w)} \leq \lambda_1\right\} = P\left\{w : \frac{Q(w)}{P(w)} < \lambda\right\}$ then $P\left\{w : \frac{Q(w)}{P(w)} \leq \lambda_1\right\} < \alpha$ and we have strict inequality $P\left\{w : \frac{Q(w)}{P(w)} < \lambda\right\} < \alpha$, which leads to a strict inequality in (b) above.

C. Proof of the sup formula (greater λ)

For $\lambda_1 > \lambda$ we have:

$$\begin{aligned} \sum_{w \in W} \min(Q(w), \lambda_1 P(w)) &= Q\{w : Q(w) < \lambda P(w)\} + Q\{w : \lambda P(w) \leq Q(w) \leq \lambda_1 P(w)\} + \lambda_1 P\{w : Q(w) > \lambda_1 P(w)\} \\ &\stackrel{(a)}{\leq} Q\{w : Q(w) < \lambda P(w)\} + \lambda_1 P\{w : \lambda P(w) \leq Q(w) \leq \lambda_1 P(w)\} + \lambda_1 P\{w : Q(w) > \lambda_1 P(w)\} \\ &= Q\{w : Q(w) < \lambda P(w)\} + \lambda_1 P\{w : Q(w) \geq \lambda P(w)\} \end{aligned}$$

where (a) follow upper bounding $Q(w)$ with $\lambda_1 P(w)$.

$$\begin{aligned}
& \sum_{w \in W} \min(Q(w), \lambda_1 P(w)) - \sum_{w \in W} \min(Q(w), \lambda P(w)) \\
& \leq Q\{w : Q(w) < \lambda P(w)\} + \lambda_1 P\{w : Q(w) \geq \lambda P(w)\} - Q\{w : Q(w) < \lambda P(w)\} - \lambda P\{w : Q(w) \geq \lambda P(w)\} \\
& = (\lambda_1 - \lambda) P\{w : Q(w) \geq \lambda P(w)\} \\
& \leq (\lambda_1 - \lambda) (1 - \alpha)
\end{aligned}$$

Since $\lambda_1 - \lambda > 0$ and $P\{w : Q(w) \geq \lambda P(w)\} \leq 1 - \alpha$, we have:

$$\sum_{w \in W} \min(Q(w), \lambda_1 P(w)) - \lambda_1 (1 - \alpha) \leq \sum_{w \in W} \min(Q(w), \lambda P(w)) - \lambda (1 - \alpha)$$

If λ_1 does not satisfy the condition (6), then $P\left\{w : \frac{Q(w)}{P(w)} < \lambda\right\} < P\left\{w : \frac{Q(w)}{P(w)} < \lambda_1\right\}$ and we are finished because there exist w_0 with $P(w_0) > 0$, $\frac{Q(w_0)}{P(w_0)} \geq \lambda$, and $\frac{Q(w_0)}{P(w_0)} < \lambda_1$, which gives strict inequality in (a) above.

APPENDIX B GENERALIZED FARKAS LEMMA

Lemma 4 (Farkas). *Let $a_i \in \mathbb{R}^n, i = 1, \dots, m$ and $b \in \mathbb{R}^n$. If for all $\mu \in \mathbb{R}^n$ such that $\mu^T \cdot a_i \geq 0$ implies $\mu^T \cdot b \geq 0$, then $b = \sum_j \lambda_j a_j$ with $\lambda_j \geq 0$.*

We need to prove the following generalization of this result:

Lemma 5 (Generalized Farkas). *Let $a_i \in \mathbb{R}^n, i = 1, \dots, m$, $b \in \mathbb{R}^n$ and $\alpha_j \geq 0$. Assume that for all $\mu \in \mathbb{R}^n$ such that $\mu^T \cdot C \geq 0$,*

$$\mu^T \cdot \left(b - \sum_j \alpha_j a_j \mathbb{1}_{\{\mu^T \cdot a_j < 0\}} \right) \geq 0 \tag{30}$$

Then: $b = \sum_j \lambda_j a_j + C \cdot \tau$ with $0 \leq \lambda_j \leq \alpha_j$.

We defer the proof of the lemma after proving the following:

Lemma 6. *Let:*

$$\eta(\mu) = \mu^T \cdot \left(b - \sum_j \alpha_j a_j \mathbb{1}_{\{\mu^T \cdot a_j < 0\}} \right) \tag{31}$$

Then minimization of $\eta(\mu)$ such that $\mu^T \cdot C \geq 0$, is equivalent to the following linear program:

$$\min \begin{pmatrix} \mu \\ z \end{pmatrix}^T \cdot \begin{pmatrix} b \\ \alpha \end{pmatrix} \text{ s.t. } \begin{pmatrix} \mu \\ z \end{pmatrix}^T \cdot \begin{pmatrix} A & 0 & C \\ I & I & 0 \end{pmatrix} \geq 0 \tag{32}$$

where A is the matrix with columns a_i , λ is a vector with entries λ_i , and α is a vector with entries α_i .

Remark 2. Obviously, 0 is an admissible solution. when there exists μ with $\eta(\mu) < 0$ then η is not bounded from below since we can multiply the solution by any positive factor. When the solution is bounded from below then it must be 0.

Proof: For each μ such that $\mu^T \cdot C \geq 0$, let $z_{opt}(\mu) = \max(0, -\mu^T \cdot A)$. Then:

$$\begin{pmatrix} \mu \\ z_{opt}(\mu) \end{pmatrix}^T \cdot \begin{pmatrix} A & 0 & C \\ I & I & 0 \end{pmatrix} \geq 0$$

and:

$$\begin{aligned}
\begin{pmatrix} \mu \\ z_{opt} \end{pmatrix}^T \cdot \begin{pmatrix} b \\ \alpha \end{pmatrix} &= \mu^T \cdot b - \sum_{j: \mu^T \cdot a_j < 0} \alpha_j (\mu^T \cdot a_j) \\
&= \mu^T \cdot \left(b - \sum_j \alpha_j a_j \mathbb{1}_{\{\mu^T \cdot a_j < 0\}} \right)
\end{aligned}$$

On the other hand, if:

$$\begin{pmatrix} \mu \\ z \end{pmatrix}^T \cdot \begin{pmatrix} A & 0 & C \\ I & I & 0 \end{pmatrix} \geq 0$$

then:

$$z \geq z_{opt}(\mu)$$

and:

$$\begin{pmatrix} \mu \\ z \end{pmatrix}^T \cdot \begin{pmatrix} b \\ \alpha \end{pmatrix} \geq \begin{pmatrix} \mu \\ z_{opt}(\mu) \end{pmatrix}^T \cdot \begin{pmatrix} b \\ \alpha \end{pmatrix} = \mu^T \cdot \left(b - \sum_j \alpha_j a_j \mathbb{1}_{\{\mu^T \cdot a_j < 0\}} \right)$$

since $\alpha \geq 0$. ■

Proof of Lemma 5: By Lemma 6, the problem is equivalent to the linear program (32). If 0 is the minimal solution, then this is equivalent to:

$$\begin{pmatrix} \mu \\ z \end{pmatrix}^T \cdot \begin{pmatrix} A & 0 & C \\ I & I & 0 \end{pmatrix} \geq 0 \Rightarrow \begin{pmatrix} \mu \\ z \end{pmatrix}^T \cdot \begin{pmatrix} b \\ \alpha \end{pmatrix} \geq 0 \quad (33)$$

Now, the standard Farkas lemma (4), this implies that there exists $\lambda = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \tau \end{pmatrix} \geq 0$ such that: $\begin{pmatrix} A & 0 & C \\ I & I & 0 \end{pmatrix} \cdot \lambda = \begin{pmatrix} b \\ \alpha \end{pmatrix}$

which is equivalent to: $A \cdot \lambda_1 + C \cdot \tau = b$ and $\lambda_1 + \lambda_2 = \alpha$, which together give $0 \leq \lambda_1 \leq \alpha$ as needed. ■

Remark 3. Note that we can add equality constraints on μ by adding two inequality constraints. For an equality constraint this results in an additional vector added to b without any restriction on their coefficient. Specifically, in our case we have the additional constraint that $\sum_{\mathbf{x}} \mu(\mathbf{x}) = 0$, which is equivalent to $\mu^T \cdot \mathbf{1} = 0$, where $\mathbf{1}$ is the vector of all ones. In Lemma 3 we obtain:

$$b = \sum_y \lambda_y a_y + \tau \mathbf{1}, \lambda_y \geq 0$$

where we don't have restrictions on τ (using the notation there).

APPENDIX C MODIFICATION FOR DMC

In this section we assume the reader is familiar with the *method of types* [7], [8]. We use standard type notation, e.g.[8]. Specifically, for a fixed n :

- $\mathbf{x} \in \mathcal{X}^n$ and $\mathbf{y} \in \mathcal{Y}^n$
- $P_{\mathbf{x}}$ denotes the empirical distribution of the sequence $\mathbf{x} \in \mathcal{X}^n$. $P_{\mathbf{x}, \mathbf{y}}$ denotes the empirical distribution of the sequence $(\mathbf{x}, \mathbf{y}) \in (\mathcal{X} \times \mathcal{Y})^n$
- $T_{\mathbf{x}}$ denotes the type class of the sequence \mathbf{x} , i.e.:

$$T_{\mathbf{x}} = \{\mathbf{x}' \in \mathcal{X}^n : P_{\mathbf{x}'} = P_{\mathbf{x}}\}$$

- $T_{\mathbf{x}|\mathbf{y}}$ is the conditional type class of \mathbf{x} given \mathbf{y} , i.e.:

$$T_{\mathbf{x}|\mathbf{y}} = \{\mathbf{x}' \in \mathcal{X}^n : P_{\mathbf{x}', \mathbf{y}} = P_{\mathbf{x}, \mathbf{y}}\}$$

- $|\cdot|$ denote the size of a set, e.g., $|T_{\mathbf{x}}|, |T_{\mathbf{x}|\mathbf{y}}|$

For DMC, we know from [2, Theorem 20] that we can restrict both the input and output distributions, as $Q_X(\mathbf{x})$ and $Q_Y(\mathbf{y})$ to be uniform on types. Using the same argument for $\gamma(Q_X, \mathbf{z})$, i.e., the convexity and concavity with respect to Q_X and \mathbf{z} shows that we can also prove that $Q_X(\mathbf{x})$ and \mathbf{z} are uniform over type. In this appendix we provide the necessary modification for the algorithm needed. Specifically, for each input type class $T_{\mathbf{x}}$ let $\lambda_{T_{\mathbf{x}}} = Q_X(T_{\mathbf{x}})$, i.e. $\lambda_{T_{\mathbf{x}}}$ is the weight of the type class $T_{\mathbf{x}}$. We have:

$$\sum_{T_{\mathbf{x}}} \lambda_{T_{\mathbf{x}}} = 1$$

and:

$$Q_X(\mathbf{x}) = \frac{\lambda_{T_{\mathbf{x}}}}{|T_{\mathbf{x}}|} \quad (34)$$

where (34) is by the uniform type assumption. We also assume that $\mathbf{z}_{\mathbf{y}}$ is fixed for each $\mathbf{y}' \in T_{\mathbf{y}}$, i.e. $\mathbf{z}_{\mathbf{y}} = \mathbf{z}_{T_{\mathbf{y}}}$. The algorithm is modified to calculate the score using $\lambda_{T_{\mathbf{x}}}$ and $\mathbf{z}_{\mathbf{y}}$ instead of $Q_X(\mathbf{x})$ and $\mathbf{z}_{\mathbf{y}}$. The linear inequality and the score function has

to be modified to incorporate λ_{T_x} and \mathbf{z}_y instead of $Q_X(\mathbf{x})$ and \mathbf{z}_y . For the linear inequality:

$$\begin{aligned} Q_X \{W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y\} &= \sum_{\mathbf{x}: W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y} Q_X(\mathbf{x}) \\ &= \sum_{\mathbf{x}: W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y} \frac{\lambda_{T_x}}{|T_x|} \\ &\stackrel{(a)}{=} \sum_{T_{x|y}: W_{Y|X}(\mathbf{y}|\mathbf{x}) > \mathbf{z}_y} \lambda_{T_x} \frac{|T_{x|y}|}{|T_x|} \end{aligned}$$

where in (a) we sum over the conditional type of \mathbf{x} given \mathbf{y} , which satisfies the condition. The condition with \geq instead of $>$ is similar. The score function:

$$\begin{aligned} \gamma(Q_X, \mathbf{z}) &= \sum_{\mathbf{x}, \mathbf{y}} Q_X(\mathbf{x}) \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y) - e^{-R} \sum_{\mathbf{y}} \mathbf{z}_y \\ &\stackrel{(b)}{=} \sum_{T_{x,y}} |T_{x,y}| Q_X(\mathbf{x}) \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y) - e^{-R} \sum_{T_y} |T_y| \mathbf{z}_y \\ &= \sum_{T_{x,y}} |T_{x,y}| \frac{\lambda_{T_x}}{|T_x|} \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y) - e^{-R} \sum_{T_y} |T_y| \mathbf{z}_y \\ &\stackrel{(c)}{=} \sum_{T_{x,y}} |T_y| \lambda_{T_x} \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y) - e^{-R} \sum_{T_y} |T_y| \mathbf{z}_y \end{aligned}$$

where (b) follows by summing over all (\mathbf{x}, \mathbf{y}) in the type class $T_{x,y}$, since $\sum_{\mathbf{x}} Q_X(\mathbf{x}) \min(W_{Y|X}(\mathbf{y}|\mathbf{x}), \mathbf{z}_y)$ is constant over the type class, and the same argument for the second sum (c) follows since $\frac{|T_{x,y}|}{|T_x|} = |T_y|$.

A few comments are in order:

Remark 4.

- Since we expect e^{-R} to be small, this suggests that calculations should be done in the log domain. This is left for further research.
- It is well known that the linear programs are harder when degeneracy occurs. This follows in our case too; had we assumed that no degeneracy occurs, some simplifications are possible. However, since we are interested in small examples, simulation results show that degeneracy does occur and we have to handle these cases as well.
- Incremental algorithm starting from large R for which the uniform distribution is optimal and reducing R while keeping optimality of the distribution Q_X through small correction to the distribution.

REFERENCES

- [1] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *Information Theory, IEEE Transactions on*, vol. 56, no. 5, pp. 2307–2359, 2010.
- [2] Y. Polyanskiy, "Saddle point in the minimax converse for channel coding," *Information Theory, IEEE Transactions on*, vol. 59, no. 5, pp. 2576–2595, 2013.
- [3] N. Elkayam and M. Feder, "Achievable and converse bounds over a general channel and general decoding metric," *arXiv preprint arXiv:1411.0319*, 2014. [Online]. Available: <http://www.eng.tau.ac.il/~elkayam/FiniteBlockLen.pdf>
- [4] —. (2016) Variational formulas for the power of the binary hypothesis testing problem with applications. [Online]. Available: http://www.eng.tau.ac.il/~elkayam/Binary_ISIT.pdf
- [5] K. Fan, "Minimax theorems," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 39, no. 1, p. 42, 1953.
- [6] W. Matthews, "A linear program for the finite block length converse of polyanskiy–poor–verdú via nonsignaling codes," *Information Theory, IEEE Transactions on*, vol. 58, no. 12, pp. 7036–7044, 2012.
- [7] I. Csiszár, "The method of types [information theory]," *Information Theory, IEEE Transactions on*, vol. 44, no. 6, pp. 2505–2523, 1998.
- [8] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011. [Online]. Available: <http://books.google.co.il/books?id=2gsLkQlb8JAC>